AO 106 (Rev. 04/10) Application for a Search Warrant

ORIGINAL

UNITED STATES DISTRICT COURT

for the

Northern District of Texas

U.S. DISTRICT COURT NORTHERN DISTRICT OF TEXAS FILED FEB 22 2021

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

angelaam85@yahoo.com

Case No. 4:21-MJ-093

FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

angelaam85@yahoo.com fully described in Attachment A.

located in the Northern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §2252, 18 U.S.C. § 2252A	Receipt of Child Pornography

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Noel Jones, HSI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 2/22/21

Judge's signature

City and state: Fort Worth, Texas

Jeffrey L. Cureton, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Noel R. Jones, being duly sworn under oath, do hereby depose and state:

INTRODUCTION

1. I am a Special Agent of the United States Department of Homeland Security, Homeland Security Investigations (HSI), and I have been employed in this capacity since December 2003. I am a graduate of the Criminal Investigator Training Program and the U.S. Immigration and Customs Enforcement Special Agent Training Academy. As a result of my employment with HSI, my duties include, but are not limited to, the investigation and enforcement of Titles 8, 18, 19, 21 and 31 of the United States Code (U.S.C.). I am an "investigative or law enforcement officer of the United States" within the meaning defined in 18 U.S.C. § 2510(7), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

2. As part of my duties as an HSI agent, I investigate crimes relating to the sexual exploitation of children, including the transportation, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. I have received training in the area of child exploitation, and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in several child pornography investigations and am familiar with the tactics used by individuals who collect and distribute child pornographic material.

3. This affidavit is being made in support of an application for a search warrant authorizing the search of information and records associated with user account and email address **angelaam85@yahoo.com**, as further described in Attachment A, that is stored at the premises owned, maintained, controlled, and operated by Oath Holdings Inc. (hereinafter referred as Oath), headquartered at 701 First Avenue, Sunnyvale, California 94089. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), and Federal Rules of Criminal Procedure Rule 41, to require Oath to disclose to the government records and other information in its possession pertaining to the subscriber(s) or customer(s) associated with the account **angelaam85@yahoo.com**, including the contents of communications, as further set forth in Attachment B.

4. In my training and experience, I am aware that Oath is a company which provides free web-based internet electronic mail ("email") access to the general public, and that stored electronic communications, including opened and unopened email for Yahoo! Mail subscribers may be located on servers or other digital devices within Oath's custody and control. Further, I am aware that computers at Oath contain information and other stored electronic Oath accounts allow users to engage in instant messaging, in which users may "chat" in real time with other users and exchange files with other users. Accordingly, this affidavit and application for a search warrant seeks authorization to search the computer accounts and/or files described herein, using the procedures described in Attachment B.

5. The statements included in this affidavit are based in part on an investigation I have conducted, as well as information provided to me by other law enforcement officers. As detailed below, I believe that the user of the electronic mail account of **angelaam85@yahoo.com**, has violated federal law, including violations of 18 U.S.C. §§ 2252A(a)(1), 2252A(a)(2) and 2252A(a)(5)(B), relating to the transportation, distribution, receipt and possession of child pornography.

6. Because this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me regarding this investigation. I have included only those facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1), 2252A(a)(2) and 2252A(a)(5)(B) are presently located in the Oath records associated with user account **angelaam85@yahoo.com.**

DEFINITIONS

7. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and the attachments incorporated herein:

a. "Internet Service Providers" (ISPs) are commercial organizations that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet, including telephone based dial-up, satellite-based internet access, dedicated circuitry, or broadband-based access via a digital subscriber line (DSL) or cable television lines. ISPs typically charge a fee, based upon the volume of data, commonly referred to as bandwidth, in addition to the type of connection that the connection supports. Many ISPs assign each subscriber an account name, such as a user name or screen

name, as well as an email address and an email mailbox, and the subscriber typically creates a password for the subscriber account. By using a computer equipped with a telephone (dial-up) or cable modem, the subscriber can establish communication with the ISP, and can access the Internet by means of a combination of the user account name and password.

b. "Internet Protocol address" or "IP address" refers to a unique number used by a computer or electronic device to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

c. "Electronic Mail," commonly referred to as email (or e-mail), is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Email systems are based on a store-and-forward model; that is, email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an email server, for as long a period of time as it takes to send or receive messages. An Internet email message generally consists of three components: the message envelope, the message header, and the message body; in some cases, it may include a fourth component, an attachment. Email attachments can include any type of digital file. There are numerous methods of obtaining an email account; some of these include email accounts issued by an employer or an education authority. One of the most commons methods of obtaining an email account is through a free web-based email service provider such as, Outlook, Yahoo!, or Gmail. Anyone with access to the Internet can generally obtain a free web-based email account.

d. The term "communication channel" means a medium through which a message can be transmitted to its intended audience, such as a print media or electronic media (e.g., oral communications or broadcast). In account subscriptions, it refers to a means of delivering account information or other messages to a customer, like email, telephone communication, or facsimile.

e. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, both visually or aurally, and by any means,

whether in handmade form (including, but not limited to: writings, drawings, and paintings), photographic form (including, but not limited to: microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to: phonograph records, printing, or typing), or electrical, electronic, or magnetic form (including, but not limited to: tape recordings, cassettes, compact discs, electronic, or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks or DVD's, Personal Digital Assistants (PDAs), Multimedia Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

INFORMATION REGARDING YAHOO! MAIL

8. Oath is a U.S.-based, multinational technology company that provides a variety of Internet-related services and products. Examples of popular Oath services include Yahoo! Mail, Yahoo! Messenger, Yahoo! Answers, Yahoo! Finance and the Yahoo! search engine.

9. Yahoo! Mail is a webmail service that allows account holders to send, receive, and store emails and attached digital files on Oath's servers, or within other Oath Account service applications. Such emails and digital files can include photographs, videos, documents, email text, and structured data (i.e., contacts and calendar items). Yahoo! Mail subscribers may obtain email accounts with the "yahoo.com" domain name.

10. During the account registration process, Oath asks subscribers to provide basic personal information. Based on my training and experience in cyber-related investigations, I am aware that Oath stores and maintains electronic communications and information about subscribers of their services, including their email service. This

information includes account access information, email transaction information, and account application information. This information may constitute evidence of the crimes under investigation as it may contain information that will identify the party in control of the subject account.

11. Oath allows account holders to access their files, which are stored on Oath's servers, from any digital device that can access the Yahoo! Mail account application's website (i.e., internet accessible devices). Oath provides free storage, up to 1TB, that can be used to store content on any of the Yahoo! applications, including Yahoo! Mail. Your affiant submits that evidence directly relating to evidence of violations of federal law, as well as the identity of the individual(s) who use a Yahoo! account, may be found in the information maintained on Oath's server(s).

FACTS IN SUPPORT OF PROBABLE CAUSE

12. In April 2019, Homeland Security Investigations (HSI) New York Special Agents (SA) initiated an investigation targeting a dark net website which focused on selling / distributing child exploitative material (CEM) and child pornography, referred to herein as "Website A[1]." Website A is a Dark web hidden service that advertises packs of child pornography images and videos sold for a fee. Examples include:

a. "FIVEpackCP of 13 Videos * CP"
b. "*6756 photos * naked children 9-15 years"
c. "five-pack-cp_s3"
d. "* 462 videos * CP"

[1] The real name of Website A is known to law enforcement, but is being disguised in order to protect the ongoing investigation.

13. Additionally, the message on the home page of Website A states: "This site contains a collection of immoral materials for acquaintance and satisfaction of sick fantasies. If you know what it is and against it, just leave the site."

14. On April 11, 2019, HSI New York conducted an undercover purchase of "* 462 videos * CP" from Website A, which described the purchase as a "archive of 27.9 Gigabytes, a collection of immoral videos with children."

15. HSI New York paid 0.02454573 in Bitcoin (approximately $124) for the files. In the course of making the purchase, agents discovered that the site operator was using Coinbase Commerce as a payment processor, which is one known to cooperate with law enforcement and comply with federal regulations for customer reporting. After the purchase of the 462 videos, HSI New York downloaded and reviewed the contents, which all consisted of CEM and child pornography videos.

16. On July 9, 2019, HSI New York conducted an undercover purchase of "five-pack-cp_s3" from Website A, which described the purchase as "archive of 238 megabyte, a micro-collection of immoral videos with children." After purchasing the file, HSI agents downloaded and reviewed the contents. The file contained 13 videos of child pornography, all of prepubescent female children with ages ranging from infants to approximately five years old. In all of the videos, prepubescent female children were giving oral sex and/or being forced to manually sexually stimulate an adult male's erect penis.

17. On September 9, 2019, HSI New York conducted an undercover purchase of "1280x720hd_s4" from Website A, which described the purchase as an "archive of 7.83 gigabytes, a mini 1280x720HD collection of immoral videos with children." After purchasing the file, HSI agents downloaded and reviewed the contents. The file contained numerous videos of child pornography.

18. On each of the purchases from Website A and after the undercover agent sent payment, the site administrator provided a password via email to "unlock" the downloaded child pornography videos. Additionally, a receipt of the purchase was sent to this same email address from Coinbase Commerce.

19. During some of the above purchases, HSI New York agents conducted undercover email communications with the administrator of Website A. The administrator stated the passwords for the pack of child pornography videos change, but the content of these videos does not. The administrator further stated they keep track of the passwords by changing the last number listed on the pack. For example, for the pack "five-pack-cp_s3" when the administrator of the Website A changes the password it will then be labeled "five-pack-cp_s4," but the content of the pack will remain the same. I believe that this is done to avoid customers from being able to share / access the downloads without paying.

20. As described above, during the undercover purchases of child pornography videos agents learned that the site operator was using Coinbase Commerce as a payment processor. Coinbase Commerce is a non-custodial cryptocurrency solution for merchants

selling digital goods. Coinbase never controls the user's cryptocurrency or private keys, only storing the keys in an encrypted manner on the cloud. The keys are only decrypted locally on the user's machine. Coinbase does provide infrastructure for receiving payments. Specifically, it provides the merchant with web links for each of their digital products. The merchant points customers to these links, which describe the product, take basic customer information, provide a unique Bitcoin address for payment, and tell the customer how much Bitcoin to send.

21. Agents subsequently sent an administrative summons to Coinbase requesting all transaction information for payments sent to the site administrator's Coinbase Commence account for Website A. Among other information, these records include the IP address of where the digital payment originated (buyer), a general description of what hardware device was used to conduct the transaction (i.e. what type of phone, web browser, etc.), a name of what was purchased (assigned by the seller), date and time of the transaction, and a unique Transaction Hash ID.

22. According to summoned records from Coinbase Commerce and subsequent analysis of the Bitcoin blockchain, HSI New York agents learned on or about July 31, 2020, a user purchased a pack titled "vedeos-462_s23" from Website A for approximately $124.04 in U.S. dollars. This transaction was assigned "Transaction Hash" number "00a24f365d92811ac9347fcab2c1a93f4ac4685467eadc22c2ccc7d49630f01b," which is a unique number that identifies the specific transaction and cannot be duplicated for other transactions. It can be similarly described as a fingerprint of the transaction.

Additionally, Coinbase records reflected the payment was conducted utilizing an IP address of "47.190.81.60," which traced back to Frontier Communications. Agents then sent an administrative summons to Coinbase for identifying information related to the above Transaction Hash, including who sent the $124.04. Coinbase stated the payment was sent from a registered account containing the following:

a. Name: Angel Aguilar
b. SSN: xxx-xx-2355
c. Date of Birth: xx/xx/64
d. Address: 2310 Balsam Drive #B210, Arlington Texas 76006
e. ID: Texas Driver License #15302644
f. Phone Number: 214-859-0025
g. Email Address: angelaam85@yahoo.com

23. I have viewed the "vedeos-462_s13" pack which was purchased and downloaded by HSI New York agents. This pack contains the same content as "vedeos-462_s23". The reason the numbers are different was explained in paragraph 19. Below are descriptions of three videos contained with the "vedeos-462_s13" pack:

File Name	File Description
kg_Kelly_10_yo	This video depicts a nude female approximately 8 to 10 years old. The female is lying on her back at the edge of a bed. A male is seen inserting his penis into the female's mouth.
Brunette Blowjob	This video depicts a clothed female approximately 5 years old. The female is performing oral sex on a male penis.
hmmleabnd	This video depicts an approximate 5 to 7-year-old female lying on her back on a bed. The female is only wearing pink socks which go up past her knees. The female's legs are restrained with a yellow rope. The camera is focusing on the genitals of the female. The video cuts to a male sitting on top of the female who is lying on her back. The female begins to masturbate the male's penis before the male takes over the masturbation. The male ejaculates on the face of the female.

24. To activate a Coinbase account it is required to submit a photograph of an identification document. The identification document submitted for this account was a Texas Driver License for Angel AGUILAR-Montalvo. The address listed on license was 2311 Balsam Drive #H213, Arlington, Texas 76006. According to the Tarrant County Appraisal District, this address was owned by AGUILAR-Montalvo from May 2015 to June 2017.

25. Records from Coinbase Commerce indicate AGUILAR-Montalvo purchased ten additional packs from Website A. Below are the additional purchases.

Date	IP Address	Amount	Name
2020-06-23 14:14:05 UTC	76.186.170.16	$10.99	latin-pack-cp_s4
2020-06-24 02:36:53 UTC	76.186.170.16	$36.00	not_included_s11
2020-06-26 00:29:42 UTC	76.186.170.16	$56.04	vedeos-150_s26
2020-06-26 22:17:38 UTC	76.186.170.16	$57.00	vedeos-158_s25
2020-06-27 07:51:40 UTC	47.190.81.60	$45.98	not_included_-2-_s9
2020-06-28 06:33:25 UTC	47.190.81.60	$107.97	not_included_-10-_s3
2020-07-01 18:21:27 UTC	76.186.170.16	$72.00	not_included_-5-_s12
2020-07-02 07:53:11 UTC	2605:6000:8c4b:2c00:28a3:210f:aef:aa13	$88.00	not_included_-6-_s6

2020-07-04 07:39:42 UTC	47.190.81.60	$96.00	not_included_-7-_s4
2020-07-24 18:54:28 UTC	76.186.170.16	$89.96	not_included_-9-_s3

26. As part of their investigation, agents with HSI New York have been able to purchase and download several packs from Website A. In addition to the aforementioned pack purchased on July 31, 2020, HSI New York agents were able to purchase and download four additional "packs" which contain the same content as the ones purchased by AGUILAR-Montalvo. I have reviewed these "packs" and they do contain images and videos which meet the federal definition of child pornography.

27. Each purchase of a "pack" containing child pornography is linked to the Yahoo! email address **angelaam85@yahoo.com** per records received from the Coinbase Cryptocurrency Exchange. After a purchase is made, Coinbase Cryptocurrency Exchange sends an email with a receipt for the purchase of the "pack" to the email provided by the purchaser. Furthermore, each individual purchase and download of a "pack" required the site administrator to email the purchaser a unique password allowing for the extraction / "unlocking" of the downloaded encrypted files. Without this emailed password, the downloaded files could not be opened by the purchaser.

28. Additionally, based on training and experience in child exploitation investigations, your affiant is aware email is a popular method of Internet communication used by individuals who transport, receive, and distribute child pornography. Offenders

utilize email to purchase, upload, trade, and store child pornography, and to communicate with other individuals regarding the sexual exploitation of children.

29. Your affiant is also aware that individuals often keep and retain email messages for years. Your affiant knows from previous child exploitation investigations that individuals often retain email messages related to the sexual exploitation of children for extended periods of time, often for years. Most email accounts, such as those offered by Oath, do not automatically delete email messages; therefore, the user of the email account must delete the email messages. If the user does not delete the email message, it will remain in the account as long as the account is active. To ensure that the contents of the account to be searched remain intact pending the execution of this warrant, a preservation request was sent to Oath on or about February 8, 2021 for the information contained in the **angelaam85@yahoo.com**.

30. This application seeks a warrant to search all responsive records and information under the control of Oath, a provider subject to the jurisdiction of this court, regardless of where Oath has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within

Oath's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States. [2]

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

31. Your affiant anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Yahoo! to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

32. Based upon the foregoing, your affiant respectfully submits that there is probable cause to believe that evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1), 2252A(a)(2) and 2252A(a)(5)(B), relating to the transportation, distribution, receipt and possession of child pornography, are contained in the Oath account **angelaam85@yahoo.com**. In consideration of the foregoing, your affiant respectfully requests that this Court issue an order authorizing the search of the Oath

[2] It is possible Oath stores some portion of the information sought outside of the United States. In *Microsoft Corp. v. United States*, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information— including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of Oath. The government also seeks the disclosure of the physical location or locations where the information is stored.

account **angelaam85@yahoo.com**, more particularly described in Attachment A, for the items, materials, and records more specifically identified in Attachment B.

33. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court (including a magistrate judge of such a court) of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

34. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Noel R. Jones
Special Agent
Homeland Security Investigations

Sworn to before me, and subscribed in my presence on this 22nd day of February 2021 at 1:30 p.m., in Fort Worth, Texas.

JEFFREY L. CURETON
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF ITEMS TO BE SEARCHED

This warrant applies to information associated with the Yahoo! email and communication account **angelaam85@yahoo.com**, including email, communication, and messenger accounts, that is stored at premises owned, maintained, controlled, or operated by Oath Holdings Inc., a company headquartered at 701 First Avenue, Sunnyvale, California 94089.

ATTACHMENT B
DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

In order to ensure that agents search only those computer accounts and/or computer files described herein, this search warrant seeks authorization to permit employees of Yahoo!, Inc. to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts and/or computer files described below, the following procedures have been implemented:

1. The warrant will be presented to Yahoo!, Inc. personnel by law enforcement agents. Yahoo!, Inc. personnel will be directed to isolate those accounts and files described below;

2. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files associated with **angelaam85@yahoo.com**, including an exact duplicate of all information stored in the computer accounts and/or files described below;

3. Yahoo!, Inc. system administrators will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and /or files to the Special Agent who serves this search warrant;

4. Yahoo!, Inc., will disclose responsive data by sending to the following recipient using the U.S. Postal Service or another courier service, notwithstanding 18 U.S.C. §§ 2252, 2252A or similar statute or code: HSI Special Agent Noel R. Jones, 125 E. John Carpenter Fwy., #750, Irving, Texas 75062.

5. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the system administrator and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant; and

6. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the system administrator, and will not further review the original duplicate absent an order of the Court.

I. Information to be disclosed by Oath Holdings Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Oath, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Oath, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Oath is required to disclose the following information to the government for each account or identifier with **angelaam85@yahoo.com**:

a. The contents of all emails stored in the account, from the time of account creation to present, including stored or preserved copies of emails sent to and from the account, email attachments, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. The contents of all Instant Messages (IM) associated with the accounts, from the time of account creation to the present, including stored or preserved copies of IMs sent to and from the account, IM attachments, draft IMs, the source and destination addresses associated with each IM, the date and time at which each IM was sent, and the size and length of each IM;

c. Any deleted emails, including any information described in subparagraph "a" above;

d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

f. All content in the Docs, Calendar, Friend Contacts and Photos areas;

g. Any and all Yahoo! IDs listed on the subscriber's Friends list;

h. All records pertaining to communications between Yahoo!, Inc. and any person regarding the account, including contacts with support services and records of actions taken;

i. All records preserved following the preservation request issued on or about February 8, 2021 for **angelaam85@yahoo.com**.

II. Information to be seized by the Government

1. All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, messenger logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1), (a)(2)(A), and (a)(5)(B), including, for each account or identifier listed on Attachment A, information pertaining to the following matters, including attempting and conspiring to engage in the following matters:

a. Any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct;

b. Any person knowingly transporting, receiving, distributing, or possessing child pornography, as defined at 18 U.S.C. § 2256(8);

2. Credit card and other financial information including but not limited to bills and payment records;

3. Evidence of the identity of the individual(s) who used, owned, or controlled the account or identifier listed on Attachment A;

4. Evidence of the times the account or identifier listed on Attachment A was used; and

5. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A and other associated accounts.